PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-152713
(43)Date of publication of application : 23.05.2003

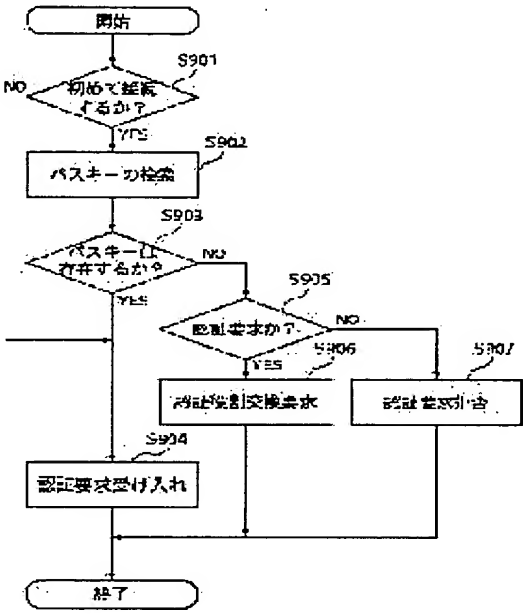
(51)Int.Cl. H04L 9/32
G06F 15/00

(21)Application number : 2001-350006
(22)Date of filing : 15.11.2001

(71)Applicant : CANON INC
(72)Inventor : FUJITA SHIGERU

(54) METHOD FOR AUTHENTICATING COMMUNICATION OPPOSITE PARTY, INFORMATION COMMUNICATION SYSTEM, AND CONTROL PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method for authenticating communication opposite parties by which even information communication devices unable to receive authentication information required to authenticate the communication opposite party can conduct authentication processing.
SOLUTION: In the case that an information communication device acting like an authentication side receives its own password and an address and an information communication device acting like a side to be authenticated receives the password and the address of the information communication device acting like the authentication side to conduct the authentication processing, the information communication device acting like the authentication side registers in advance passwords and addresses of information communication devices to be communication opposite parties, and when the information communication device acting like the authentication side becomes an information communication device acting like the side to be authenticated, the information communication device acting like the authentication side becoming the information communication device acting like the side to be authenticated uses the password and the address having been stored in advance of an information communication device acting like the authentication side to conduct the authentication processing. Further, when the own device has no function of receiving a password and an address of an information communication device at the authentication side in spite of it that the own device becomes the side to be authenticated and stores no password nor address, the own device responds it to the information communication device acting like at present the authentication side that the own device changes the roll to act like the authentication side.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than

THIS PAGE LEFT BLANK

the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

THIS PAGE LEFT BLANK

(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開２００３－１５２７１３
（Ｐ２００３－１５２７１３Ａ）
(43)公開日　平成15年5月23日(2003.5.23)

(51)Int.Cl.⁷	識別記号	FI			テーマコード(参考)
Ｈ０４Ｌ　9/32		Ｇ０６Ｆ　15/00	３３０	Ｃ	5B085
Ｇ０６Ｆ　15/00	３３０	Ｈ０４Ｌ　9/00	６７３	Ａ	5J104

審査請求　未請求　請求項の数２３　ＯＬ　（全１３頁）

(21)出願番号　特願2001-350006(P2001-350006)

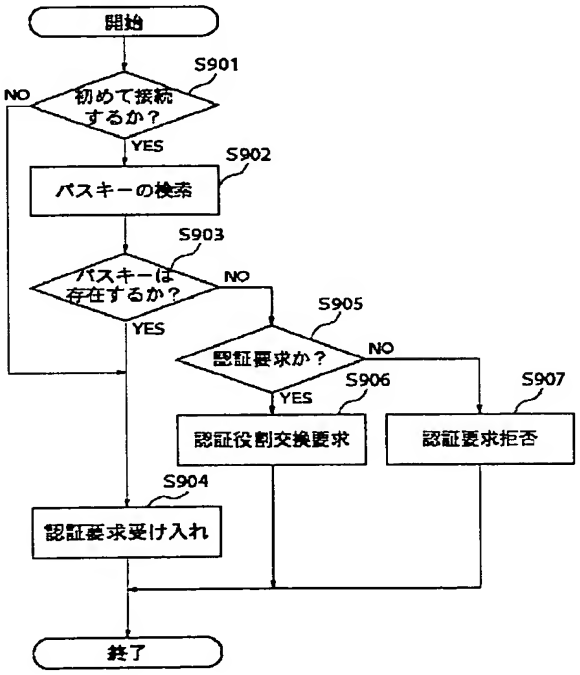
(22)出願日　平成13年11月15日(2001.11.15)

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子3丁目30番2号
(72)発明者　藤田　茂
東京都大田区下丸子3丁目30番2号　キヤノン株式会社内
(74)代理人　100081880
弁理士　渡部　敏彦

Ｆターム(参考)　5B085 AE04
5J104 AA07 EA03 KA02

(54)【発明の名称】通信相手認証方法、情報通信システム、及び制御プログラム

(57)【要約】
【課題】　通信相手を認証するのに必要な認証情報を入力できない情報通信装置同士でも認証処理を行えるようにする。
【解決手段】　認証側となる情報通信装置は自己のパスワードとアドレスを入力し、被認証側となる情報通信装置は認証側となる情報通信装置のパスワードとアドレスを入力することにより認証処理を行う場合に、通信相手となり得る情報通信装置のパスワードとアドレスを予め登録しておき、自装置が被認証側となった場合は、予め記憶しておいた認証側の情報通信装置のパスワードとアドレスを使用して認証処理を遂行する。また、自装置が被認証側となったにも拘わらず、自装置が該認証側の情報通信装置のパスワードとアドレスを入力する機能を持たず、かつパスワードとアドレス記憶していないときは、役割を交代して自装置が認証側になる旨の応答を現在認証側となっている情報通信装置に対して行う。



【特許請求の範囲】

【請求項１】　通信を開始する際に通信相手となる情報通信装置を認証する通信相手認証方法であって、
被認証側となる情報通信装置は、認証側となる情報通信装置の認証情報を該被認証側となる情報通信装置が直接読み取り可能な記憶媒体に予め記憶しておき、認証処理の際には、記憶しておいた認証情報を使用して認証手続きを行うことを特徴とする通信相手認証方法。

【請求項２】　前記通信相手認証方法は、認証側となる情報通信装置は、自己の認証情報を入力し、被認証側となる情報通信装置は認証側となる情報通信装置の認証情報を入力することにより、認証処理を遂行することを特徴とする請求項１に記載の通信相手認証方法。

【請求項３】　前記被認証側となる情報通信装置は、前記認証側となる情報通信装置から認証要求が発させられた場合に、自装置が該認証側となる情報通信装置の認証情報を入力する機能を持たず、かつ該認証情報を前記記憶媒体に記憶していないときは、自装置が認証側になる旨の応答を現在認証側となっている情報通信装置に対して行うことを特徴とする請求項１又は２に記載の通信相手認証方法。

【請求項４】　前記認証情報は、パスワード情報とアドレス情報であることを特徴とする請求項１～３の何れかに記載の通信相手認証方法。

【請求項５】　前記認証側となる情報通信装置と、被認証側となる情報通信装置は、前記認証情報の１つとして自装置のアドレス情報を予め記憶していることを特徴とする請求項１～４の何れかに記載の通信相手認証方法。

【請求項６】　前記認証処理は、所定の規格の無線通信を行う場合に実行されることを特徴とする請求項１～５の何れかに記載の通信相手認証方法。

【請求項７】　前記所定の規格の無線通信は、ｂｌｕｅｔｏｏｔｈ規格の無線通信であることを特徴とする請求項６に記載の通信相手認証方法。

【請求項８】　前記記憶媒体は、前記被認証側となる情報通信装置に予め内蔵された記憶媒体であることを特徴とする請求項１～７の何れかに記載の通信相手認証方法。

【請求項９】　前記被認証側となる情報通信装置は、該被認証側となる情報通信装置にケーブルで接続された情報通信装置から前記認証側となる情報通信装置の認証情報を取得して前記予め内蔵された記憶媒体に記憶することを特徴とする請求項８に記載の通信相手認証方法。

【請求項１０】　前記記憶媒体は、前記被認証側となる情報通信装置に着脱自在な記憶媒体であることを特徴とする請求項１～７の何れかに記載の通信相手認証方法。

【請求項１１】　前記被認証側となる情報通信装置は、前記記憶媒体に予め記憶しておいた認証側となる情報通信装置の認証情報を使用して認証処理を行って通信した場合は、当該認証側となる情報通信装置へのリンク情報

を記憶しておき、当該認証側となる情報通信装置から再度認証要求がなされた際には、該リンク情報を検索することにより該認証要求を受理することを特徴とする請求項１～１０の何れかに記載の通信相手認証方法。

【請求項１２】　通信相手となる情報通信装置を認証した後に通信を開始する情報通信システムであって、
被認証側となる情報通信装置は、認証側となる情報通信装置の認証情報を該被認証側となる情報通信装置が直接読み取り可能な記憶媒体に予め記憶しておき、認証処理の際には、記憶しておいた認証情報を使用して認証手続きを行うことを特徴とする情報通信システム。

【請求項１３】　前記認証処理は、認証側となる情報通信装置は、自己の認証情報を入力し、被認証側となる情報通信装置は認証側となる情報通信装置の認証情報を入力することにより、認証処理を遂行するものであることを特徴とする請求項１２に記載の情報通信システム。

【請求項１４】　前記被認証側となる情報通信装置は、前記認証側となる情報通信装置から認証要求が発させられた場合に、自装置が該認証側となる情報通信装置の認証情報を入力する機能を持たず、かつ該認証情報を前記記憶媒体に記憶していないときは、自装置が認証側になる旨の応答を現在認証側となっている情報通信装置に対して行うことを特徴とする請求項１２又は１３に記載の情報通信システム。

【請求項１５】　前記認証情報は、パスワード情報とアドレス情報であることを特徴とする請求項１２～１４の何れかに記載の情報通信システム。

【請求項１６】　前記認証側となる情報通信装置と、被認証側となる情報通信装置は、前記認証情報の１つとして自装置のアドレス情報を予め記憶していることを特徴とする請求項１２～１５の何れかに記載の情報通信システム。

【請求項１７】　前記認証処理は、所定の規格の無線通信を行う場合に実行されることを特徴とする請求項１２～１６の何れかに記載の情報通信システム。

【請求項１８】　前記所定の規格の無線通信は、ｂｌｕｅｔｏｏｔｈ規格の無線通信であることを特徴とする請求項１７に記載の情報通信システム。

【請求項１９】　前記記憶媒体は、前記被認証側となる情報通信装置に予め内蔵された記憶媒体であることを特徴とする請求項１２～１８の何れかに記載の情報通信システム。

【請求項２０】　前記被認証側となる情報通信装置は、該被認証側となる情報通信装置にケーブルで接続された情報通信装置から前記認証側となる情報通信装置の認証情報を取得して前記予め内蔵された記憶媒体に記憶することを特徴とする請求項１９に記載の情報通信システム。

【請求項２１】　前記記憶媒体は、前記被認証側となる情報通信装置に着脱自在な記憶媒体であることを特徴と

する請求項１２～１８の何れかに記載の情報通信システム。

【請求項２２】　前記被認証側となる情報通信装置は、前記記憶媒体に予め記憶しておいた認証側となる情報通信装置の認証情報を使用して認証処理を行って通信した場合は、当該認証側となる情報通信装置へのリンク情報を記憶しておき、当該認証側となる情報通信装置から再度認証要求がなされた際には、該リンク情報を検索することにより該認証要求を受理することを特徴とする請求項１２～２１の何れかに記載の情報通信システム。

【請求項２３】　通信相手となる情報通信装置を認証した後に通信を開始する情報通信システムにおいて被認証側となる情報通信装置により実行される制御プログラムであって、
認証側となる情報通信装置から認証要求がなされた場合に、該認証要求を受けて被認証側となる情報通信装置は、該被認証側となる情報通信装置が直接読み取り可能な記憶媒体に予め記憶しておいた認証側となる情報通信装置の認証情報を読み出し、該読み出した認証情報を使用して認証手続きを行う内容を有することを特徴とする制御プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報通信機器間における通信相手の認証技術に関する。

【０００２】

【従来の技術】従来、情報機器同士が通信を行う際、最も簡便な場合は、通信相手が如何なる機器であっても接続・通信を許可していた。しかし、複数の機器を対象に通信を行いたい場合、接続相手機器を識別してアクセス権を管理し、セキュリティを確保するために、ユーザＩＤとパスワードを用いて管理・運用する方法が広く用いられてきた。

【０００３】近年、普及の著しいインターネットにおいては、ユーザＩＤとパスワードによるアクセス管理が広く一般に行われている。ユーザは、ネットワーク接続時にユーザＩＤとパスワード情報を送信し、認証されると通信を開始できるようになる。

【０００４】サーバ・クライアントモデルのネットワークでは、サーバ側にユーザＩＤとパスワードを記録・管理しておき、クライアントから接続要求が来た時に送られてくるユーザＩＤとパスワード情報を照合し、適合していればアクセス権を付与し、通信を開始するよう構成されている。ユーザが初めて通信を行う時は、予めユーザ情報をサーバ側に設定しておくか、ゲストアカウントで接続した後、ユーザＩＤ、パスワードをクライアント端末側から送信し、サーバ側に設定するよう構成されている。

【０００５】また、近年、ネットワークの物理媒体として電波を用いる無線ネットワークが普及してきている。無線ネットワークにおいても、サーバ・クライアントモデル・ネットワークは、上記と同様のアクセス権の管理が行われている。

【０００６】このようなアクセス権の管理機能が、Ｂｌｕｅｔｏｏｔｈに代表されるような近距離無線ネットワーク機器、特に携帯機器に実装される場合、使用される場所を選ばないので、今までに一度も接続したことのない機器同士が通信をする機会が増えることが予想される。また、無線通信なので、いつ、どの機器同士が接続しているのかがユーザには判り難く、通信していることに気付かない間にユーザの情報が盗まれる等の被害を防ぐためには、強固なセキュリティの実現が重要となる。

【０００７】Ｂｌｅｕｔｏｏｔｈ規格では、上記セキュリティの問題に対応するため、機器間の接続通信前に認証を行う方法が考慮されている。Ｂｌｕｅｔｏｏｔｈ規格におけるリンクレイヤーの機器認証の動作を以下に示す。

【０００８】機器認証は、１対１の機器間で行われる。図１０を参照しながら詳細を説明する。図１０は、Ｂｌｕｅｔｏｏｔｈ機能を搭載した２つの端末ＡとＢの間での認証処理時のやりとりと各端末内部で実行される処理について時系列順に表したものである。図１０の上部から下部へ向かって時間が経過するものとする。図１０の左側の実線の左側が端末Ａ内部を、右側の実線の右側が端末Ｂ内部を表している。図１０の中央の実線と実線の間の破線矢印が、端末Ａと端末Ｂ間の電波による情報通信を示している。

【０００９】通信接続時に端末Ａ、端末Ｂのどちらかが、通信相手を認証する認証側或いは被認証側として、認証プロセスを起動し、認証手続きの開始を要求する。ここでは、ユーザＡが端末Ａをユーザ Ｂが端末Ｂを操作するものとする。

【００１０】図１０では端末Ａが通信相手を認証する認証側、端末Ｂが通信相手として認証される被認証側となり、端末Ａがステップ Ｓ５０１で認証要求を端末Ｂへ送り、認証プロセスを起動する。端末Ｂはステップ Ｓ５０２で認証受付応答を返し、認証手続きを開始する。ステップ Ｓ５０３では、端末Ａ内部で生成した乱数１（５３１）を端末Ｂへ送信する一方、端末Ａ自身の持つＢｌｕｅｔｏｏｔｈパスキー（以下パスキー）と呼ばれる文字列または数字列を端末Ａのユーザ Ａに入力させる。

【００１１】パスキーとは、Ｂｌｕｅｔｏｏｔｈ対応端末が持つ機器固有のパスワード情報であり、今まで接続したことのない、言い換えると初めて接続する端末と認証手続きを行う際に使用される情報である。入力されたパスキーＡ（５３２）とパスキーＡの長さであるパスキーＡ長（５３３）を演算アルゴリズム１Ａ（５３４）の入力として使用する。

【００１２】演算アルゴリズム１Ａ（５３４）は、初期化キー生成アルゴリズムであり、端末Ａ内部で実行さ

れ、鍵情報である初期化キー１Ａ（５３８）を生成する。乱数１（５３１）を受け取った端末Ｂ内部では、端末Ａ同様、ユーザＢに端末Ａのパスキー Ａを入力させ、入力されたパスキーＡ（５３５）とパスキーＡの長さであるパスキーＡ長（５３６）を演算アルゴリズム１Ｂ（５３７）の入力として使用する。

【００１３】なお、端末Ａに対してユーザＡが入力するパスキーＡ（５３２）と端末Ｂに対してユーザＢが入力するパスキーＡ（５３５）は同一であるべきものである。換言すれば、被認証側が認証側のパスキーを正しく入力することを条件として、被認証側を認証側の通信相手として認証するのである。

【００１４】従って、パスキーＡ長（５３３）とパスキーＡ長（５３６）も同一となるべきものである。また、端末Ｂ内部で実行される演算アルゴリズム１Ｂ（５３７）と端末Ａ内部で実行される演算アルゴリズム１Ａ（５３４）も、同一のアルゴリズムである。端末Ｂでも端末Ａと同様に初期化キー１Ｂ（５３９）が生成されるが、これも端末Ａで生成される初期化キー１Ａ（５３８）と同一となるべきものである。

【００１５】次に、端末Ａは乱数１（５３１）とは異なる乱数２（５４０）を生成し、ステップＳ５０４において端末Ｂへ送信する。また、上記乱数２（５４０）、上記初期化キー１Ａ（５３８）と被認証側である端末ＢのＢｌｕｅｔｏｏｔｈ Ｄｅｖｉｃｅ Ａｄｄｒｅｓｓ（以下ＢＤ＿ＡＤＤＲ＿Ｂ）（５４１）を演算アルゴリズム２Ａ（５４２）の入力として使用し、演算結果Ａ（５４５）を得る。

【００１６】演算アルゴリズム２Ａ（５４２）は、接続認証アルゴリズムであり、端末Ａ内部で実行される。なお、ＢＤ＿ＡＤＤＲ＿Ｂは各Ｂｌｕｅｔｏｏｔｈ機器固有のアドレス番号であり、かつ認証手続き処理を開始する前段階、すなわちステップＳ５０１を実行する前に、機器同士が接続を確立する際に交換する情報に含まれているので、この時点では既知の情報となっている。

【００１７】乱数２（５４０）を受け取った端末Ｂ内部では、端末Ａ同様、乱数２（５４０）、上記初期化キー１Ｂ（５３９）と端末ＢのＢＤ＿ＡＤＤＲ＿Ｂ（５４３）を演算アルゴリズム２Ｂ（５４４）の入力として使用し、演算結果Ｂ（５４６）を得る。端末Ｂ内部で実行される演算アルゴリズム２Ｂ（５４４）と端末Ａ内部で実行される演算アルゴリズム２Ａ（５４２）は、同一のアルゴリズムである。また、端末Ａで使用するＢＤ＿ＡＤＤＲ＿Ｂ（５４１）と、端末Ｂで使用するで使用するＢＤ＿ＡＤＤＲ＿Ｂ（５４３）は、同一の情報である。

【００１８】次に、端末Ｂは、ステップＳ５０５において、演算結果Ｂ（５４６）を端末Ａへ送信する。端末Ａでは、ステップＳ５０６Ａにおいて、端末Ａ自身の内部で演算・生成した演算結果Ａ（５４５）と、端末Ｂ内部で演算・生成されて端末Ｂから送信された演算結果Ｂ（５４６）とを比較する。演算結果Ａと演算結果Ｂの値が等しければ、認証は成功とし、値が異なると認証は失敗とする。認証が成功すると、端末Ｂを正当な通信相手として認証し、次の通信処理へと進む。また、認証に失敗した場合は、接続を切断して処理を終了する。

【００１９】なお、セキュリティレベルをより高めるため、認証成功後、端末Ａと端末Ｂの認証役割を交換、すなわち、今度は端末Ａが被認証側、端末Ｂが認証側となり、端末Ｂで生成する乱数と端末Ｂの持つパスキーＢと端末ＡのＢＤ＿ＡＤＤＲ＿Ａをパラメータとして、図１０と同様の手続きで認証を行い、端末相互で認証処理を行うことも可能である。ただし、上記役割を交換して行う認識処理は、省略可能である。

【００２０】上述した認証動作は、通信を行う双方の端末共にユーザがパスキーを入力可能な場合であるが、Ｂｌｕｅｔｏｏｔｈを搭載した機器の中にはユーザがパスキーを入力することが困難であるか、又は入力できない機器も存在する。

【００２１】このような機器の場合、固定パスキーを予め機器内蔵のメモリに設定しておき、認証時に通信相手端末のユーザに前記固定パスキーの入力を促し、自分のパスキーは前記固定パスキーを内蔵メモリから読み出して使用することによって、パスキー入力不能な機器のユーザがパスキーを入力しなくても良い方法が考慮されている。

【００２２】この例を図１１に基づいて説明する。なお、図１１の例では、端末Ａがパスキー入力可能な端末、端末Ｃがパスキー入力不能な端末となっている。また、図１１の表現方法は、図１０と同様である。

【００２３】ステップＳ６０１で、端末Ａが認証側として認証要求を端末Ｃへ送り、認証プロセスを起動する。端末Ｃにおいてはユーザ Ｃがパスキーを入力することができないので、ステップＳ６０２で、被認証側として認証プロセスを実行することを拒否し、端末Ａに対して認証側と被認証側との役割を交換し、端末Ｃが認証側となることを要求する認証役割交換要求を送信する。

【００２４】端末Ａにおいてはユーザ Ａがパスキーを入力することができるので、端末Ｃからの認証役割交換要求を受け付けて、ステップＳ６０３で認証受付応答を返し、認証手続きを開始する。このとき、図１１に示したように、端末Ａは被認証側、端末Ｃは認証側に役割が交換される。この後は、図１０のステップＳ５０３以降の処理と同等の処理が、端末Ａが被認証側、端末Ｃが認証側として行われる。ただし、この場合、端末Ｃは、予め端末Ｃ内に設定されている、図示しない固定パスキーＣを演算アルゴリズム１Ｃへの入力に使用する点が異なる。

【００２５】次に、通信を行う双方の端末共にユーザがパスキーを入力できない機器、すなわち固定パスキーを持つ機器同士の場合の認証手続き例を、図１２に基づい

て説明する。図１２の表現方法は図１０と同様である。

【００２６】ステップＳ７０１で、端末Ｃが認証側として認証要求を端末Ｄへ送り、認証プロセスを起動する。端末Ｄは、パスキーを入力することができないので、ステップＳ７０２で、被認証側として認証プロセスを実行することを拒否し、端末Ｃに対して認証側と被認証側との役割を交換し端末Ｃが認証側となることを要求する認証役割交換要求を送信する。

【００２７】しかし、端末Ｃでもユーザがパスキーを入力することができないので、認証役割交換要求を受け付けることができず、ステップＳ７０３で、役割交換拒否応答を端末Ｄへ返す。この時点で、端末Ｃ、端末Ｄが共に被認証側になることを拒否し合ったため、認証手続きを開始することができず、通信を切断するよう動作していた。

【００２８】

【発明が解決しようとする課題】上述したように、従来のＢｌｕｅｔｏｏｔｈ規格における機器接続時の認証方法では、ユーザがパスキーを入力できない機器同士を認証処理実行後に接続しようとすると、どちらの機器も機器内に記憶してある固定パスキーを認証に使用し、被認証側ではなく認証側となって認証手続きを行おうとするので、認証手続きの役割分担が成立せず、結果として接続・通信することができないという欠点があった。従って、ユーザにとっては機器の使い勝手が非常に悪くなっていた。

【００２９】本発明は、このような従来技術の問題に鑑みてなされたもので、その課題は、通信相手を認証するのに必要な認証情報を入力できない情報通信装置同士でも認証処理を行えるようにすることにある。

【００３０】

【課題を解決するための手段】上記課題を解決するため、本発明は、通信を開始する際に通信相手となる情報通信装置を認証する通信相手認証方法であって、被認証側となる情報通信装置は、認証側となる情報通信装置の認証情報を該被認証側となる情報通信装置が直接読み取り可能な記憶媒体に予め記憶しておき、認証処理の際には、記憶しておいた認証情報を使用して認証手続きを行うように構成されている。

【００３１】また、本発明は、通信相手となる情報通信装置を認証した後に通信を開始する情報通信システムであって、被認証側となる情報通信装置は、認証側となる情報通信装置の認証情報を該被認証側となる情報通信装置が直接読み取り可能な記憶媒体に予め記憶しておき、認証処理の際には、記憶しておいた認証情報を使用して認証手続きを行うように構成されている。

【００３２】また、本発明は、通信相手となる情報通信装置を認証した後に通信を開始する情報通信システムにおいて被認証側となる情報通信装置により実行される制御プログラムであって、認証側となる情報通信装置から認証要求がなされた場合に、該認証要求を受けて被認証側となる情報通信装置は、該被認証側となる情報通信装置が直接読み取り可能な記憶媒体に予め記憶しておいた認証側となる情報通信装置の認証情報を読み出し、該読み出した認証情報を使用して認証手続きを行う内容を有している。

【００３３】

【発明の実施の形態】以下、本発明の実施の形態を、図面に基づいて詳細に説明する。

【００３４】［第１の実施形態］図１は、本発明の第１実施形態に係るＢｌｕｅｔｏｏｔｈ機能を搭載したデジタルカメラのブロック図、図２は、Ｂｌｕｅｔｏｏｔｈ機能を搭載したプリンタのブロック図である。本実施形態に係るプリンタは、パスキーの入力手段を持たない機器であり、固定パスキーを本体内に記憶している。本実施形態に係るデジタルカメラは、外部機器から本デジタルカメラ内のメモリに予め書き込んでおいた接続通信相手（プリンタ）のＢＤ＿ＡＤＤＲとパスキーを読み出して、認証処理時に使用するように構成されている。

【００３５】図１に示すデジタルカメラ１００は、ＣＰＵ１０１、ＲＯＭ１０２、ＲＡＭ１０３、不揮発性メモリ１０４、ワイヤレス通信回路部１０５、アンテナ１０６、外部機器接続コネクタ１０７、インタフェース回路部１０８、撮像部１０９、操作部１１０、表示部１１１、及び２次記憶部１１２を有しており、図示するように、内部バス１１３によって相互に接続されている。また、デジタルカメラ１００は、電源回路部１１４を備え、前記各ブロックに電源ライン１１５によって電源を供給する。

【００３６】ＣＰＵ１０１は、ＲＯＭ１０２に格納されているプログラムに従って動作し、デジタルカメラの各種動作を制御する。ＲＯＭ１０２はデジタルカメラの制御手順（図４，５，７，１０に対応する制御プログラムを含む）等を予め格納した不揮発性メモリである。ＲＡＭ１０３は撮像部１０９から出力されるデジタル画像データの一時的なバッファリング、２次記憶部１１２へ書き込むデータや、２次記憶部から読み出したデータの一時的な記憶、ＣＰＵ１０１の演算等に使用するワークエリア、ワイヤレス通信回路部から送受信される通信データ、各種設定等を一時的に格納するエリアとして使用される。

【００３７】不揮発性メモリ１０４は、書き換え可能であり、機器の各種設定やＢｌｕｅｔｏｏｔｈ通信に使用する通信相手ＢＤ＿ＡＤＤＲ、以前接続したＢｌｕｅｔｏｏｔｈ機器との通信に使用するリンクキー情報等を記憶・保存する。ワイヤレス通信回路部１０５は、ワイヤレス通信に必要な高周波回路部、符号化・複合化回路部、無線通信時に使用するＦＩＦＯメモリ、自身のＢＤ＿ＡＤＤＲ＿Ｄ、自身のパスキーＤを記憶している不揮発性メモリ等から構成され、アンテナ１０６が接続され

ている。

【００３８】外部機器接続コネクタ１０７は、外部機器とデジタルカメラ１００を接続するコネクタである。インタフェース回路部１０８は、外部機器接続コネクタ１０７を介して接続された外部機器との間でデータ通信を行う機能を備えている。ＣＰＵ１０１の制御に従い、外部機器へのデータの送信及び外部機器からのデータの受信を行う。

【００３９】撮像部１０９は、入射する光を結像するレンズ、結像した光を電気信号へ変換する光電変換器（ＣＣＤやＣＭＯＳセンサ等）、光電変換器から出力されるアナログ電気信号をデジタル電気信号へ変換するＡＤコンバータ（アナログ－デジタル変換器）等から成る。操作部１１０は、図示しない撮影を指示するレリーズボタン、デジタルカメラ１００の動作モードを選択するモード選択ダイヤル、メニュー項目を呼び出すメニューボタン、メニュー項目を選択・指示する十字カーソルボタン等のボタン、ダイヤル、スイッチで構成され、これらボタン、ダイヤル、スイッチの状態及び状態変化を電気信号として出力する。

【００４０】表示部１１１は、液晶表示装置等で構成され、デジタルカメラ１００の動作状態や撮影した画像データを表示する。２次記憶部１１２は撮影したデジタル画像データ等を格納する。電源回路部１１４はバッテリ、ＤＣ／ＤＣコンバータ等で構成され、前述した各ブロックへ電源を供給する。

【００４１】図２に示すプリンタ２００は、ＣＰＵ２０１、ＲＯＭ２０２、ＲＡＭ２０３、不揮発性メモリ２０４、ワイヤレス通信回路部２０５、アンテナ２０６、外部機器接続コネクタ２０７、インタフェース回路部２０８、印刷部２０９、操作部２１０、表示部２１１を有しており、図示するように内部バス２１２によって相互に接続されている。また、プリンタ２００は電源回路部２１３を備え、前記各ブロックに電源ライン２１４によって電源を供給する。

【００４２】ＣＰＵ２０１は、ＲＯＭ２０２に格納されているプログラムに従って動作し、プリンタの各種動作を制御する。ＲＯＭ２０２はプリンタの制御手順（図４，５，７，１０に対応する制御プログラムを含む）、フォントデータ等を予め格納した不揮発性メモリである。ＲＡＭ２０３は外部機器から送信される印刷用データの一時的なバッファリング、印刷部へ送るデータへの変換作業用のワークエリア、ＣＰＵ１０１の演算等に使用するワークエリア、ワイヤレス通信回路部から送受信される通信データ、各種設定等を一時的に格納するエリアとして使用される。

【００４３】不揮発性メモリ２０４は、書き換え可能であり、機器の各種設定やＢｌｕｅｔｏｏｔｈ通信に使用する通信相手ＢＤ＿ＡＤＤＲ、以前接続したＢｌｕｅｔｏｏｔｈ機器との通信に使用するリンクキー情報等を記憶・保存する。ワイヤレス通信回路部２０５は、ワイヤレス通信に必要な高周波回路部、符号化・複合化回路部、無線通信時に使用するＦＩＦＯメモリ、自身のＢＤ＿ＡＤＤＲ＿Ｐ、自身のパスキーＰを記憶している不揮発性メモリ等から構成され、アンテナ２０６が接続されている。

【００４４】外部機器接続コネクタ２０７は、外部機器とプリンタ２００を接続するコネクタである。インタフェース回路部２０８は、外部機器接続コネクタ２０７を介して接続された外部機器との間でデータ通信を行う機能を備えている。ＣＰＵ２０１の制御に従い、外部機器へのデータの送信及び外部機器からのデータの受信を行う。

【００４５】印刷部２０９は印刷データを紙へ印刷するための印刷ヘッド、印刷ヘッド駆動モータ、紙搬送ローラ、紙搬送ギア駆動モータ、ギア等からなるプリントエンジン部である。操作部２１０は、図示しないプリンタの電源ＯＮ・ＯＦＦを指示する電源ボタン、リセットボタン等で構成され、これらボタン等の状態及び状態変化を電気信号として出力する。表示部２１１はＬＥＤランプ等で構成され、プリンタ２００の動作状態等を示す。電源回路部２１３はＡＣ／ＤＣコンバータ、ＤＣ／ＤＣコンバータ等で構成され、前述した各ブロックへ電源を供給する。

【００４６】第１の実施形態に係るデジタルカメラ１００は、パスキー入力機能の無い機器（プリンタ）との間で認証処理を行うために、以下の設定が行われる。すなわち、図１に示すデジタルカメラ１００の外部機器接続コネクタ１０７にパーソナルコンピュータをケーブルで接続し、予め調べておいたプリンタ２００のＢｌｕｅｔｏｏｔｈアドレス（ＢＤ＿ＡＤＤＲ＿Ｐ）とプリンタ２００のパスキー情報（パスキーＰ）をリスト情報として、デジタルカメラ１００の２次記憶部１１２の所定のエリアに書き込んでおく。

【００４７】図３に、２次記憶部１１２内に格納されているパスキーリスト（１２０１）の例を示す。ＢＤ＿ＡＤＤＲとパスキーがペアとして格納されている。図３では［ＢＤ＿ＡＤＤＲ＿Ｐ（１２０２）、パスキーＰ（１２０３）］、［ＢＤ＿ＡＤＤＲ＿Ｒ（１２０４）、パスキーＲ（１２０５）］の２つのペアを持っている。ここでは２つのペアのパスキーリストを例示したが、ペアの個数に特に制限はない。

【００４８】次に、デジタルカメラ１００とプリンタ２００の間で行うＢｌｕｅｔｏｏｔｈ通信の認証処理を、図面に基づいて詳細に説明する。

【００４９】図４は、プリンタ２００が認証側、デジタルカメラ１００が被認証側として認証手続きを行う場合の認証処理を示した図である。

【００５０】プリンタ２００がデジタルカメラ１００に対して認証手続きを要求する（ステップＳ８０１）。プ

リンタ２００からの認証要求を受け取ったデジタルカメラ１００は、パスキー検索処理（８３１）を実行する。パスキー検索処理（８３１）の結果、プリンタ２００のＢＤ＿ＡＤＤＲ＿Ｐ、パスキーＰが存在する場合、認証要求受付応答を、存在しない場合被認証側としての認証要求は受け付けず、プリンタ２００に対して認証側と被認証側との役割を交換し、デジタルカメラ１００が認証側となることを要求する認証役割交換要求を応答として送信する（ステップＳ８０２）。

【００５１】次に、図４中に示したパスキー検索処理（８３１）の詳細を、図５に基づいて説明する。なお、図５は、処理内容を一般化して示しているが、ここでは、今までの説明で用いた例に沿って説明する。

【００５２】まず、認証要求を送信してきたプリンタ２００が今回初めて接続する相手かどうかを判断する（ステップＳ９０１）。具体的には、デジタルカメラ１００の不揮発性メモリ１０４中に記憶されている機器接続リストの中に、プリンタ２００のＢＤ＿ＡＤＤＲ＿Ｐに合致するＢＤ＿ＡＤＤＲと、接続に必要なリンクキーＰがリストアップされているかどうかを検索する。リストアップされていなければ、初めて接続する機器であるのでステップＳ９０２へ進み、リストアップされていれば、ステップＳ９０４へ進む。

【００５３】図６に機器接続リストの例を示す。ＢＤ＿ＡＤＤＲと前回認証接続時に生成したＬＩＮＫ ＫＥＹをペアとしたリスト（１１０１）として格納されている。図６には、［ＢＤ＿ＡＤＤＲ＿Ａ（１１０２）、ＫＥＹ＿Ａ（１１０３）］、［ＢＤ＿ＡＤＤＲ＿Ｆ（１１０４）、ＫＥＹ＿Ｆ（１１０５）］、［ＢＤ＿ＡＤＤＲ＿Ｚ（１１０６）、ＫＥＹ＿Ｚ（１１０７）］の３つのペアが記憶されており、ステップＳ９０１において、この機器接続リスト１１０１の中からプリンタ２００のＢＤ＿ＡＤＤＲであるＢＤ＿ＡＤＤＲ＿Ｐを検索し、有るか否かを判定する。図６の機器接続リスト１１０１には、ＢＤ＿ＡＤＤＲ＿Ｐが登録されていないので、プリンタ２００は初めて接続する機器と判断され、ステップＳ９０２へ進むことになる。

【００５４】次に、デジタルカメラ１００の２次記憶部１１２に格納されたパスキーリスト１２０１の中に、プリンタ２００のＢＤ＿ＡＤＤＲ＿ＰとパスキーＰがリストアップされているかどうかを検索する（ステップＳ９０２）。そして、プリンタ２００のＢＤ＿ＡＤＤＲ＿Ｐ（１２０２）に対応するパスキーＰ（１２０３）がリストアップされているか否かを判定する（ステップＳ９０３）。パスキーＰが存在すればステップＳ９０４へ進み、存在しなければステップＳ９０５へ進む。

【００５５】ステップＳ９０４では、プリンタ２００へ返す応答として、認証要求受け入れを選択する。 ステップＳ９０５では、パスキー検索処理８３１を起動する要因が、認証要求か否かを判定する。その結果、認証要求であった場合はステップＳ９０６へ進み、認証役割交換要求であった場合はステップＳ９０７へ進む。

【００５６】ステップＳ９０６では、プリンタ２００へ返す応答として認証役割交換要求を選択し、ステップＳ９０７では、プリンタ２００へ返す応答として認証要求拒否を選択する。 ステップＳ９０４，９０６，９０７の何れかの処理を行った後、本パスキー検索処理（８３１）を終了する。

【００５７】次に、図４とは逆に、プリンタ２００が被認証側、デジタルカメラ１００が認証側となって認証手続きを行う場合の認証処理を、図７に基づいて説明する。

【００５８】ここでは、図４のように、プリンタ２００がデジタルカメラ１００に対して認証手続きを要求するのではなく、デジタルカメラ１００が認証側となってプリンタ２００に対して認証手続きを要求する（ステップＳ１００１）。デジタルカメラ１００からの認証要求を受け取ったプリンタ２００は、パスキー入力手段を持たないため、認証要求を拒否し、デジタルカメラ１００に対して認証役割交換要求を送信する（ステップＳ１００２）。

【００５９】プリンタ２００からの認証役割交換要求を受け取ったデジタルカメラ１００は、パスキー検索処理（１０３１）を実行する。ここで行うパスキー検索処理（１０３１）は、図４（図５）に示したパスキー検索処理（８３１）と同じである。パスキー検索処理（１０３１）の結果、プリンタ２００のＢＤ＿ＡＤＤＲ＿Ｐ、パスキーＰが存在する場合は、認証要求受付応答を、存在しない場合は、被認証側としての認証要求は受け付けず、プリンタ２００に認証要求拒否応答を送信する（ステップＳ１００３）。

【００６０】上述したように、第１の実施形態によれば、ユーザがパスキーを入力できないか、或いはパスキーの入力が困難な端末同士が通信開始時に認証処理を行う場合、従来は、認証手続きを実行できなかったが、本実施形態によれば、どちらか一方の端末（本実施形態においてはデジタルカメラ１００）が、外部機器によって予め本体内のメモリに設定された通信相手端末のＢＤ＿ＡＤＤＲとパスキー（本実施の形態においてはプリンタ２００のＢＤ＿ＡＤＤＲ＿ＰとパスキーＰ）を読み出して使用することにより、認証処理を行うことができる。従って、セキュリティを確保した状態で接続通信することが可能となるという効果がある。

【００６１】なお、デジタルカメラ１００に認証要求を送信してきたプリンタ２００のＢＤ＿ＡＤＤＲ＿Ｐ或いはパスキーＰが設定されていないと、デジタルカメラ１００は従来と同様、認証要求を受け入れないので、未知の機器から勝手に接続されてしまうといった危険を排除することがきる。

【００６２】さらに、予め記憶しておいたアドレスとパ

スキーを認証処理に利用するので、これらを通信開始時に入力する手間が省けると共に、迅速に認証処理を完了して通信を開始することが可能となる。また、アドレスとパスキーを入力する必要がなくなるので、例えば、本来、入力機能と通信機能を持たない種類の電子機器にも通信機能を搭載するだけで本情報通信システムを適用可能となるなど、本情報通信システムを利用し得る情報通信装置の種類を増やすことができ、利便性を向上させることが可能となる。

【００６３】［第２の実施形態］図８は、本発明の第２実施形態に係るＢｌｕｅｔｏｏｔｈ機能を搭載したデジタルカメラのブロック図、図９は、Ｂｌｕｅｔｏｏｔｈ機能を搭載したプリンタのブロック図である。第２の実施形態におけるプリンタは、パスキーの入力手段を持たない機器であり、固定パスキーを本体内に記憶している。第２の実施形態におけるデジタルカメラは、外部機器によって予め接続通信相手のＢＤ＿ＡＤＤＲとパスキーを書き込んでおいたメモリカードを装着し、認証処理時にメモリカードからパスキーを読み出して使用するものである。

【００６４】図８に示すデジタルカメラ３００は、ＣＰＵ３０１、ＲＯＭ３０２、ＲＡＭ３０３、不揮発性メモリ３０４、ワイヤレス通信回路部３０５、アンテナ３０６、撮像部３０７、操作部３０８、表示部３０９、及びメモリカード・インタフェース回路部３１０を有しており、メモリカード３１４を前記メモリカード・インタフェース回路部３１０に装着することが可能である。各ブロックは、図示するように内部バス３１１によって相互に接続されている。また、デジタルカメラ３００は電源回路部３１２を備え、前記各ブロックに電源ライン３１３によって電源を供給する。

【００６５】ＣＰＵ３０１は、ＲＯＭ３０２に格納されているプログラムに従って動作し、デジタルカメラの各種動作を制御する。ＲＯＭ３０２は、デジタルカメラの制御手順（図４，５，７，１０に対応する制御プログラムを含む）等を予め格納した不揮発性メモリである。ＲＡＭ３０３は、撮像部３０７から出力されるデジタル画像データの一時的なバッファリング、本体に装着したメモリカード３１４へ書き込むデータや、メモリカード３１４から読み出したデータの一時的な記憶、ＣＰＵ３０１の演算等に使用するワークエリア、ワイヤレス通信回路部から送受信される通信データ、各種設定等を一時的に格納するエリアとして使用される。

【００６６】不揮発性メモリ３０４は、書き換え可能であり、機器の各種設定やＢｌｕｅｔｏｏｔｈ通信に使用する通信相手のＢＤ＿ＡＤＤＲ、以前接続したＢｌｕｅｔｏｏｔｈ機器との通信に使用するリンクキー情報等を記憶・保存する。ワイヤレス通信回路部３０５は、ワイヤレス通信に必要な高周波回路部、符号化・複合化回路部、無線通信時に使用するＦＩＦＯメモリ、自身のＢＤ＿ＡＤＤＲ＿Ｄ、自身のパスキーＤを記憶している不揮発性メモリ等から構成され、アンテナ３０６が接続されている。

【００６７】撮像部３０７は、入射する光を結像するレンズ、結像した光を電気信号へ変換する光電変換器、光電変換器から出力されるアナログ電気信号をデジタル電気信号へ変換するＡＤコンバータ等から成る。操作部３０８は、図示しない撮影を指示するレリーズボタン、デジタルカメラ３００の動作モードを選択するモード選択ダイヤル、メニュー項目を呼び出すメニューボタン、メニュー項目を選択・指示する十字カーソルボタン等のボタン、ダイヤル、スイッチで構成され、これらボタン、ダイヤル、スイッチの状態及び状態変化を電気信号として出力する。

【００６８】表示部３０９は、液晶表示装置等で構成され、デジタルカメラ３００の動作状態や撮影した画像データを表示する。メモリカード・インタフェース回路部３１０は、装着されたメモリカード３１４との間でデータの読み出し、書き込み、カード装着の有無の検出等を行う機能を備えている。電源回路部３１２は、バッテリ、ＤＣ／ＤＣコンバータ等で構成され、前述した各ブロックへ電源を供給する。

【００６９】図９に示すプリンタ４００は、ＣＰＵ４０１、ＲＯＭ４０２、ＲＡＭ４０３、不揮発性メモリ４０４、ワイヤレス通信回路部４０５、アンテナ４０６、外部機器接続コネクタ４０７、インタフェース回路部４０８、印刷部４０９、操作部４１０、表示部４１１、メモリカード・インタフェース回路部４１２、及びメモリカード４１３を有しており、図示したように、内部バス４１４によって相互に接続されている。また、プリンタ４００は、電源回路部４１５を備え、前記各ブロックに電源ライン４１６によって電源を供給する。

【００７０】ＣＰＵ４０１は、ＲＯＭ４０２に格納されているプログラムに従って動作し、プリンタの各種動作を制御する。ＲＯＭ４０２はプリンタの制御手順（図４，５，７，１０に対応する制御プログラムを含む）、フォントデータ等を予め格納した不揮発性メモリである。ＲＡＭ４０３は、外部機器から送信される印刷用データの一時的なバッファリング、印刷部へ送るデータへの変換作業用のワークエリア、ＣＰＵ４０１の演算等に使用するワークエリア、ワイヤレス通信回路部から送受信される通信データ、各種設定等を一時的に格納するエリアとして使用される。

【００７１】不揮発性メモリ４０４は、書き換え可能であり、機器の各種設定やＢｌｕｅｔｏｏｔｈ通信に使用する通信相手ＢＤ＿ＡＤＤＲ、以前接続したＢｌｕｅｔｏｏｔｈ機器との通信に使用するリンクキー情報等を記憶・保存する。ワイヤレス通信回路部４０５は、ワイヤレス通信に必要な高周波回路部、符号化・複合化回路部、無線通信時に使用するＦＩＦＯメモリ、自身のＢＤ

＿ＡＤＤＲ＿Ｐ、自身のパスキーＰを記憶している不揮発性メモリ等から構成され、アンテナ４０６が接続されている。

【００７２】外部機器接続コネクタ４０７は、外部機器とプリンタ４００を接続するコネクタである。インタフェース回路部４０８は、外部機器接続コネクタ４０７を介して接続された外部機器との間でデータ通信を行う機能を備えている。ＣＰＵ４０１の制御に従い、外部機器へのデータの送信及び外部機器からのデータの受信を行う。

【００７３】印刷部４０９は、印刷データを紙へ印刷するための印刷ヘッド、印刷ヘッド駆動モータ、紙搬送ローラ、紙搬送ギア駆動モータ、ギア等からなるプリントエンジン部である。操作部４１０は、図示しないプリンタの電源ＯＮ・ＯＦＦを指示する電源ボタン、リセットボタン等で構成され、これらボタン等の状態及び状態変化を電気信号として出力する。表示部４１１はＬＥＤランプ等で構成され、プリンタ４００の動作状態等を示す。メモリカード・インタフェース回路部４１２は、装着されたメモリカード４１３との間でデータの読み出し、書き込み、カード装着の有無の検出等を行う機能を備えている。電源回路部４１５は、ＡＣ／ＤＣコンバータ、ＤＣ／ＤＣコンバータ等で構成され、前述した各ブロックへ電源を供給する。

【００７４】第２の実施形態に係るデジタルカメラ３００においても、第１の実施形態に係るデジタルカメラ１００と同様に、パスキー入力機能の無い機器（プリンタ）との間で認証処理を行うために、以下の設定が行われる。すなわち、図８に示すデジタルカメラ３００に装着可能なメモリカード３１４を、パーソナルコンピュータ等の外部機器のメモリカードスロットへ装着し、予め調べておいたプリンタ４００のＢｌｕｅｔｏｏｔｈアドレス（ＢＤ＿ＡＤＤＲ＿Ｐ）と、プリンタ４００のパスキー情報（パスキーＰ）を、メモリカード３１４の所定のエリアに書き込んでおく。

【００７５】そして、通信を行う場合は、このメモリカード３１４をデジタルカメラ３００に装着しておく。なお、メモリカード３１４内に設定されているＢＤ＿ＡＤＤＲとパスキーリストは、第１実施形態におけるデジタルカメラ１００内蔵の不揮発性メモリ１０４内のパスキーリスト１２０１（図３参照）と同様のものである。

【００７６】第２の実施形態における認証処理は、第１の実施形態と同様なので説明を省略する。ただし、第１実施形態においては、デジタルカメラがプリンタのＢＤ＿ＡＤＤＲとパスキーをデジタルカメラの２次記憶部から読み出したが、第２の実施形態においては、デジタルカメラに装着したメモリカードから読み出す点が異なる。

【００７７】従来は、ユーザがパスキーを入力できないか、或いはパスキーの入力が困難な端末同士、すなわち固定パスキーを用いる端末同士が通信開始時に認証処理を行う場合、認証手続きを実行できなかったが、第２の実施形態によれば、どちらか一方の端末（本実施形態においてはデジタルカメラ３００）が、通信相手端末のＢＤ＿ＡＤＤＲとパスキー（本実施形態においてはプリンタ４００のＢＤ＿ＡＤＤＲ＿Ｐとパスキー Ｐ）を予め外部機器によって書き込んだメモリカードを装着し、認証実行時にメモリカードから読み出して使用することにより、認証処理を行うことができる。従って、セキュリティを確保した状態で接続通信することができるようになるという効果がある。

【００７８】また、メモリカードにプリンタ４００のＢＤ＿ＡＤＤＲ＿Ｐとパスキー Ｐを格納してあるため、このメモリカードを別のＢｌｕｅｔｏｏｔｈ搭載のデジタルカメラ等に装着することにより、当該デジタルカメラ等は、プリンタ４００との間で認証処理を実行することができるようになる。

【００７９】さらに、通常はキー入力を必要としない機器は、パスキーを入力するためだけに入力手段を持つ必要がないので、コストアップを招くことなく認証処理を実行できるようになるという効果がある。

【００８０】なお、第１実施形態及び第２実施形態においては、デジタルカメラ内蔵の２次記憶部１１２またはデジタルカメラに装着可能なメモリカード３１４にプリンタのＢＤ＿ＡＤＤＲ＿Ｐとパスキー Ｐを書き込んでおき、認証実行時に使用したが、これとは逆に、プリンタ内蔵のメモリ不揮発性メモリ２０４またはプリンタに装着可能なメモリカード４１３にデジタルカメラのＢＤ＿ＡＤＤＲ＿Ｄとパスキー Ｄを書き込んでおき、認証実行時にプリンタ内でパスキー検索処理を行い、ＢＤ＿ＡＤＤＲ＿Ｄとパスキー Ｄを読み出して認証処理に使用し、第１実施形態及び第２実施形態において説明したデジタルカメラとプリンタの役割を入れ替えて動作させることも可能である。

【００８１】さらに、第１実施形態、第２実施形態では、認証実行時に使用する認証用情報としてＢｌｕｅｔｏｏｔｈパスキーを使用していたが、Ｂｌｕｅｔｏｏｔｈパスキーの代わりに異なる文字列等からなるパスワードを使用しても構わない。Ｂｌｕｅｔｏｏｔｈパスキーを使用する場合は、ネットワーク階層のリンク層で認証処理を行うが、パスワードを使用する場合は、アプリケーション層で認証処理を行うよう動作する。

【００８２】なお、Ｂｌｕｅｔｏｏｔｈパスキーを使用する場合は、上記のように、ネットワーク階層のリンク層で認証処理を行うので、アプリケーションの開発を効率よく進めることが可能となる。また、認証情報としてパスワードを使用する場合は、上記のように、アプリケーション層で認証処理を行うので、本情報通信システムに対応する情報通信装置を増やすことが可能となる。

【００８３】

【発明の効果】以上説明したように、本発明によれば、通信相手を認証するのに必要な認証情報を入力できない情報通信装置同士でも認証処理を行うことが可能となり、本情報通信システムを利用可能な情報通信装置の種類が増え、利便性が向上する。

【図面の簡単な説明】

【図１】本発明の第１実施形態におけるデジタルカメラの構成を示すブロック図である。

【図２】本発明の第１実施形態におけるプリンタの構成を示すブロック図である。

【図３】本発明の第１実施形態及び第２実施形態におけるパスキーリストの一例を示す図である。

【図４】本発明の第１実施形態及び第２の実施形態における端末間での認証要求と応答までの処理動作を示す図である。

【図５】図４の処理動作の１つであるパスキー検索処理の詳細を示すフローチャートである。

【図６】本発明の第１実施形態及び第２実施形態における機器接続リストの一例を示す図である。

【図７】本発明の第１実施形態及び第２実施形態における２つの端末間での認証要求と応答までの処理動作で、認証役割交換が行われる場合の動作を示す図である。

【図８】本発明の第２実施形態におけるデジタルカメラの構成を示すブロック図である。

【図９】本発明の第２実施形態におけるプリンタの構成を示すブロック図である。

【図１０】従来の２つの端末間における認証手続き動作を示す図である。

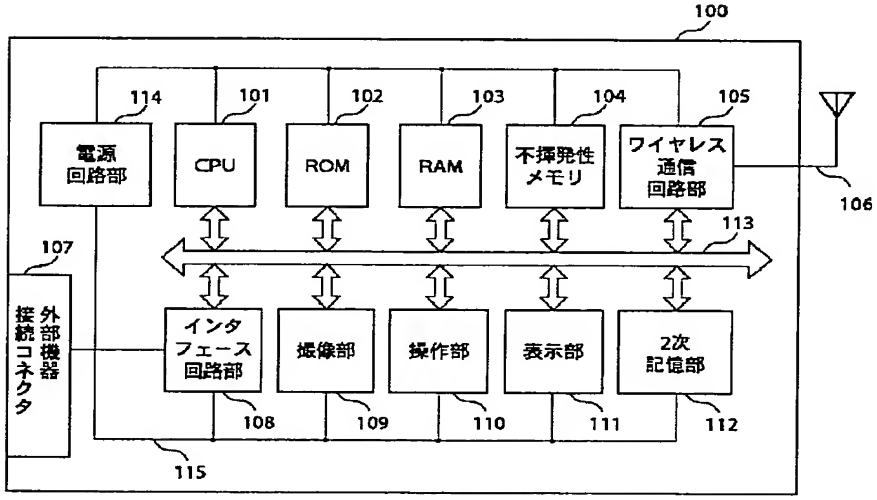
【図１１】従来の２つの端末間における認証手続き動作のうち、認証役割交換が行われる動作を示す図である。

【図１２】従来の２つの端末間における認証手続き動作のうち、認証役割交換が行われず、認証手続きが失敗し、終了する動作を示す図である。

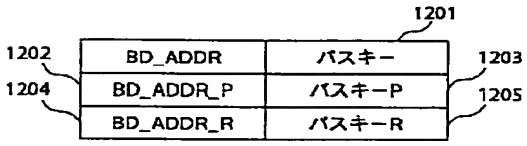
【符号の説明】

１００，３００：デジタルカメラ本体
１０１，２０１，３０１，４０１：ＣＰＵ
１０２，２０２，３０２，４０２：ＲＯＭ
１０３，２０３，３０３，４０３：ＲＡＭ
１０４，２０４，３０４，４０４：不揮発性メモリ
１０５，２０５，３０５，４０５：ワイヤレス通信回路部
１０７，２０７，３０７，４０７：外部機器接続コネクタ
１１２，２１１：２次記憶部
２００，４００：プリンタ
３１４，４１３：メモリカード
１１０１：機器接続リスト
１２０１：パスキーリスト

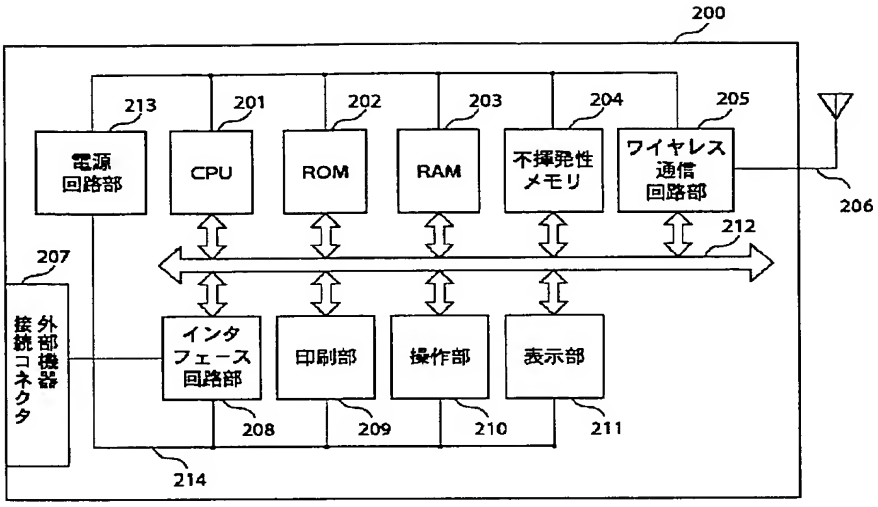
【図１】



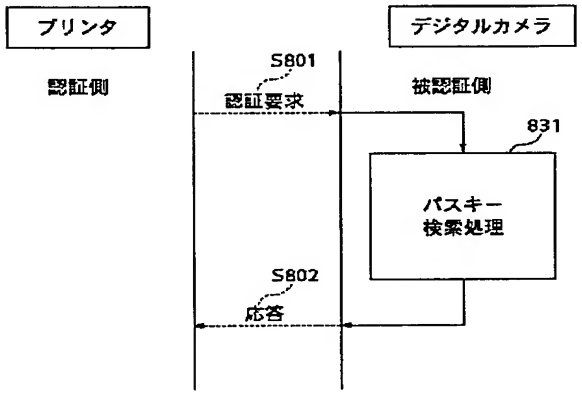
【図３】



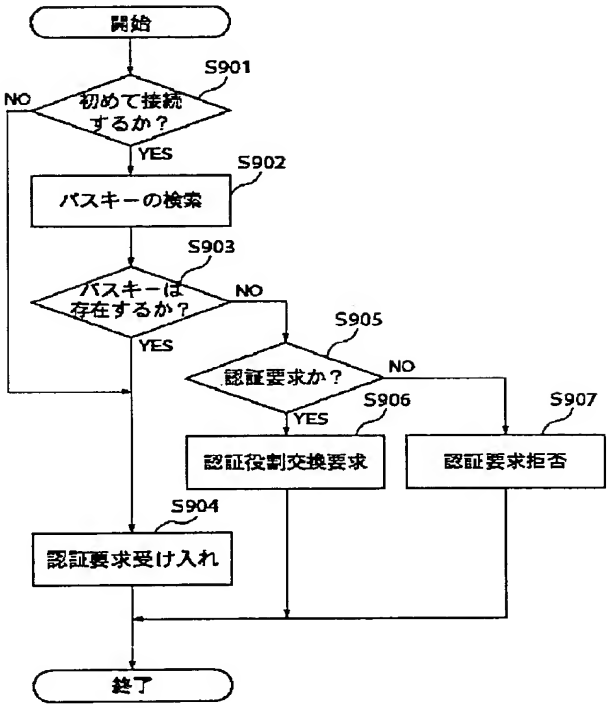
【図２】


200
213
201
202
203
204
205
電源回路部
CPU
ROM
RAM
不揮発性メモリ
ワイヤレス通信回路部
206
212
207
外部機器接続コネクタ
インタフェース回路部
印刷部
操作部
表示部
208
209
210
211
214

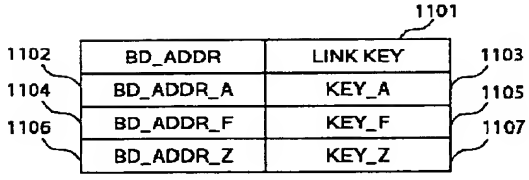
【図４】


プリンタ
デジタルカメラ
認証側
被認証側
S801
認証要求
831
パスキー検索処理
S802
応答

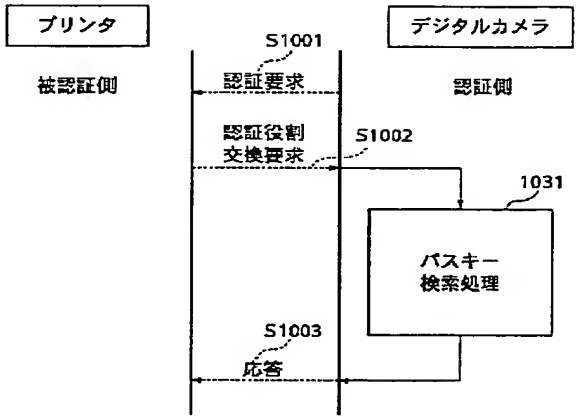
【図５】


開始
S901
初めて接続するか？
NO
YES
S902
パスキーの検索
S903
パスキーは存在するか？
NO
YES
S905
認証要求か？
NO
YES
S906
認証役割交換要求
S907
認証要求拒否
S904
認証要求受け入れ
終了

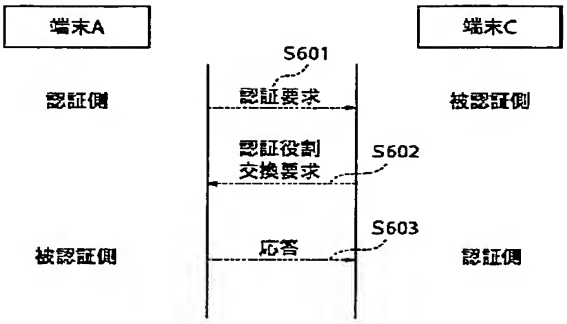
【図６】


1101
1102
BD_ADDR
LINK KEY
1103
1104
BD_ADDR_A
KEY_A
1105
1106
BD_ADDR_F
KEY_F
1107
BD_ADDR_Z
KEY_Z

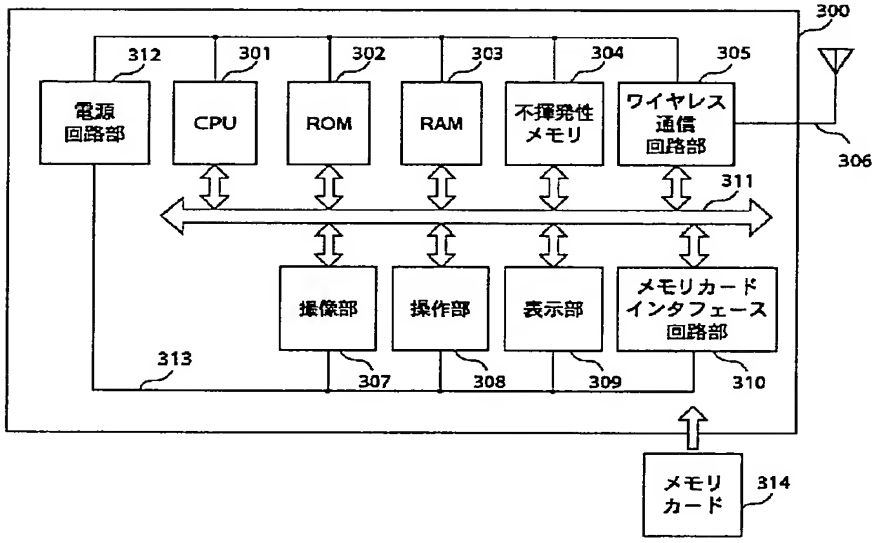
【図７】


プリンタ
被認証側
デジタルカメラ
認証側
S1001
認証要求
認証役割
交換要求
S1002
1031
バスキー
検索処理
S1003
応答

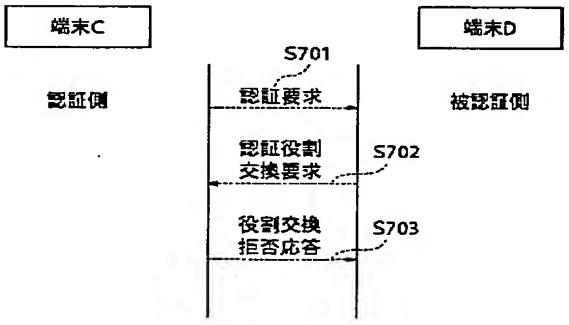
【図１１】


端末A
認証側
被認証側
端末C
S601
認証要求
認証役割
交換要求
S602
応答
S603
被認証側
認証側

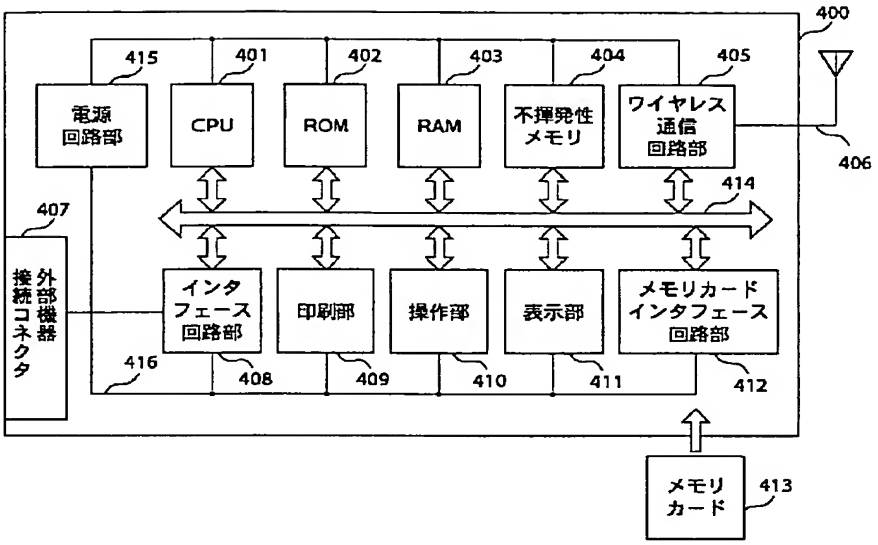
【図８】


300
312
301
302
303
304
305
電源
回路部
CPU
ROM
RAM
不揮発性
メモリ
ワイヤレス
通信
回路部
306
311
撮像部
操作部
表示部
メモリカード
インタフェース
回路部
313
307
308
309
310
メモリ
カード
314

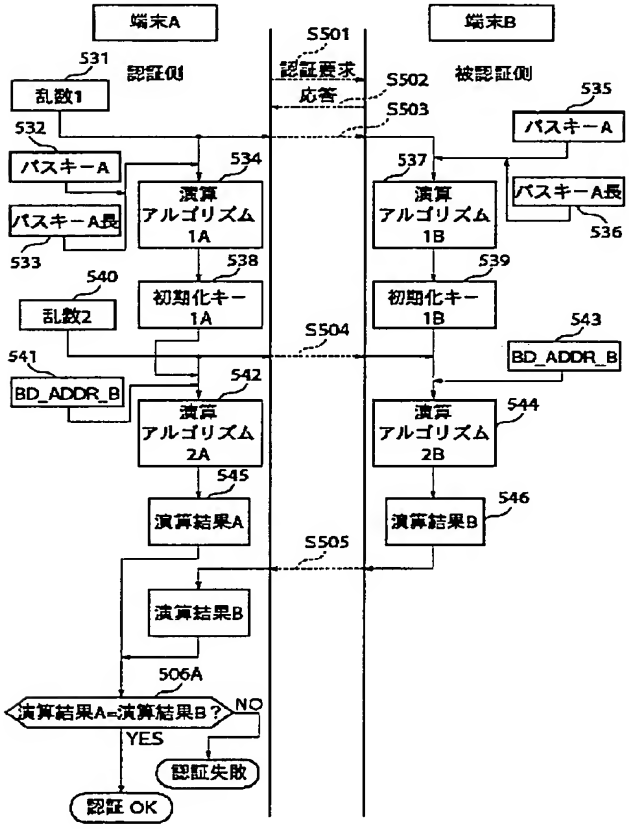
【図１２】


端末C
認証側
端末D
被認証側
S701
認証要求
認証役割
交換要求
S702
役割交換
拒否応答
S703

【図９】


400
415
401
402
403
404
405
電源回路部
CPU
ROM
RAM
不揮発性メモリ
ワイヤレス通信回路部
406
414
407
外部機器接続コネクタ
インタフェース回路部
印刷部
操作部
表示部
メモリカードインタフェース回路部
416
408
409
410
411
412
メモリカード
413

【図１０】


端末A
端末B
S501
認証要求
S502
応答
S503
S504
S505
531
認証側
被認証側
乱数1
532
パスキーA
534
演算アルゴリズム1A
パスキーA長
533
538
初期化キー1A
540
乱数2
541
BD_ADDR_B
542
演算アルゴリズム2A
545
演算結果A
535
パスキーA
537
演算アルゴリズム1B
パスキーA長
536
539
初期化キー1B
543
BD_ADDR_B
544
演算アルゴリズム2B
546
演算結果B
演算結果B
506A
演算結果A=演算結果B？
NO
YES
認証失敗
認証OK

THIS PAGE LEFT BLANK